DETAILED ACTION

1. Claims 1-7, 15, 16, and 18-19 are pending.

2. Claims 1, and 15 are amended.

Information Disclosure Statement

3. The information disclosure submitted 08/26/2009 "Australian Application Examiner's Report" is considered and an initialized copy is herein attached.

Response to Argument

Applicant's amendments and arguments filed on 4/27/09 is not persuasive.

Regarding argument's the applied references failure to teach a specific type of authentication token that includes the private key of the media player that is known to just the media player and the authentication service and a public key for the authentication service, as amended and recited on claims 1 and 15, is not persuasive because Spagna et al. teaches transmitting content and token license and the license including key 623 for decrypting the content and the key 623 being corresponding to the public key 661 of the End-User(s) and the key is only known to the clearing house and the End-User device **(see col. 95 lines 5-15 and fig. 6 e.g. element 660 of fig. 6; sc(s) processor 192 of the end-user receives the content 113, decrypting the content 113 using the key 623, i.e. "content key" (see fig. 6 for key 623 being attached on the content), and also key 623 is a "key" corresponding to public key 661** ***"it is decrypted using the Key 623 (corresponding to the Public Key 661) of the End-User(s) extracted from the license SC(s) sent from clearing house 105"*** **and therefor key 623 is a key pair, moreover key 623 is extracted from License SC(s) 660 received as a token transmitted via authenticator clearing house**

105 and the content key 623 is a key that is only known by the clearing house and the end-user device).

Moreover, the amended limitation is very well-known at the time of the invention, the examiner discloses, CHU 2003/0016829 A1, that the server generates a content private key that is only known by the server and the client and providing it to the client for content decryption; And a public key for authentication service (see par. 35 and 45 and fig. 9).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over McGarrahan et al. US Pub. 20030026424 A1. in view of Ishibashi et al. 20010053223 A1, Ishiguro et al. 7266691 B1 and Spagna et al. 6859791 B1.

As per claim 1, McGarrahan et al. method implemented in a computer-readable medium that processed on a computer to authenticate a media stream recipient (0050-0055), comprising:

automatically receiving an authentication request from a media player when a recipient attempts to use the media player to play a media stream (0050-0051 and 0054), the media stream includes the media player and media content (0032-0033) and the media content is in a format

known only to the media player (0054, 0047, 0051 and 0009 lines 11-13) and is not accessible to the recipient until the media player determines that the recipient is authenticated for access and the media player generates authentication information on behalf of the recipient and supplies that authentication information with the authentication request (0053-0054; *STB requiring key from central billing system for user request*); and wherein the media player is self-loading and self-extracting from the streamed media stream within a computing environment of the recipient (0051; *user device STB displaying content stored with in STB based on authentication result upon user request*), and self-loads and executes when the recipient attempts to use the media player to play the media content (0051-0055);

verifying that the recipient is authorized to play the media content of the media stream (0051) in response to the media player supplied and generated authentication information (0053); and

sending an authentication token to the media player over a network connection, when if the recipient is authorized (0053), and wherein the media player automatically plays the media content stream once the authentication token is received by the media player, and wherein the authentication token serves as an electronic acknowledgement that it is okay to play the media content (0051).

McGarrahan et al. fails to explicitly disclose wherein when the recipient receives the media content via the media stream the recipient receives with that media stream the media player (*media player/software, according to applicant's remark on 12/12/09, received with content at the recipient*) and the authentication information including plurality of identifiers, as amended.

However it is well known to transmit a content with a software to let the receiver/recipient device know what kind of software has been used (*see Ishibashi et al. fig. 5 for algorithms for signature..., and see fig. 12 a single stream 1200 that contains content and digital signature comprising algorithm, and see par. 0112, and 0130-0132 for verifying and providing content using the received algorithm*); and

One ordinary skill in the art would also easily understand that authentication information of McGarrahan et al. is made of plurality of identifiers but fail to include few, However Ishibashi teaches wherein the generated authentication information includes an identity for the recipient **(see Ishibashi et al. fig. 16 user ID),** an identification for the media content or media stream **(see Ishibashi et al. fig. 16 content ID),** settings for the computing device's electronic environment **(Ishibashi et al.; setting fig. 16 element 1601 i.e. user control status (UCS) for each devices in an electronic environment)**, an identification for the requesting media player **(see fig. 16 and par. 0218 UCS is provided based on device name and/or encryption processing unit ID)**, identifications for any previous sender or recipient of the media stream **(see fig. 16 user ID and fig. 21)**, and an identity of a content provider that owns the media stream **(fig. 16 content provider ID).**

Therefore it would have been obvious at the time of the invention was made to modify the teachings of Ishibashi et al. within the system of McGarrahan et al. because they are analogous in secure method of providing content. One would have been motivated to modify the teachings because it would specify what kind of software has been used and authenticate using received algorithm. And further, one would have been motivated to incorporate and modify the

teachings, as Ishibashi suggests on 0204, to include any identification information for identification purpose in the authentication process.

The combination of McGarrahan et al. and Ishibashi et al. fail to explicitly disclose wherein the media player and media content temporarily reside in volatile memory of a recipient computing device associated with the recipient and once the media content is played for the recipient the media player and content are removed from volatile memory and no longer available on the recipient computing device thereby requiring the recipient to re-acquire the media content and media player each time the media content is played by the recipient.

However Ishiguro et al. discloses providing and storing content to user device flash memory for specified time and playing content only according to the specified time, and when the specified time ends deleting the content from the user devices flash memory (see col. 23 lines 10-33 and col. 8 lines 29-33) and requiring a re-authentication and re-acquiring content re-transmission each time the user tries to replay after deletion (see col. 29 lines 3-32).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Ishiguro et al. because they are analogous in content protection. One would have been motivated to incorporate the teachings and modify it within the combination system because it would control content from being replayed illegally without controlled access.

The combination fails to disclose the authentication information including an Internet Protocol (IP) address for a recipient computing device of the recipient; and

wherein the authentication token is a key pair having a private key of the media player known only to an authentication server and the media player and having a public

key for the authentication service, wherein the authentication service is the method processing on the computer.

However Spagna et al. discloses an Internet Protocol (IP) address for a recipient computing device of the recipient (Spagna et al. see claim 16). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Spagna et al. within the combination system because they are analogous in content distribution. One would have been motivated to incorporate the teachings of Spagna et al. to identify the IP address of the recipient computing device.

Spagna et al. further discloses wherein the authentication token is a key pair having a private key of the media player known only to an authentication service and the media player and having a public key for the authentication server, wherein the authentication service is the method processing on the computer **(see col. 95 lines 5-15 and fig. 6 e.g. element 660 of fig. 6; sc(s) processor 192 of the end-user receives the content 113, decrypting the content 113 using the key 623, i.e. "content key" (see fig. 6 for key 623 being attached on the content), and also key 623 is a "key" corresponding to public key 661 *"it is decrypted using the Key 623 (corresponding to the Public Key 661) of the End-User(s) extracted from the license SC(s) sent from clearing house 105"* and therefor key 623 is a key pair, moreover key 623 is extracted from License SC(s) 660 received as a token transmitted via authenticator clearing house 105 and the content key 623 is a key that is only known by the clearing house and the end-user device).**

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to include the teachings of Spagna et al. within the combination system

to use commonly known media private key and public key of the authenticator/content provider that is very well known in the art for security, at the time of the invention was made.

As to claim 2, McGarrahan et al. discloses the method wherein the sending further comprises automatically installing the authentication token as a licensing key on a computing device of the recipient, wherein the licensing key can include licensing limitations (0053, 0055, and 0068).

As to claim 3, McGarrahan et al. discloses the method wherein in automatically receiving, the recipient initially obtains the media player and media stream from a second recipient (0048 and 0050).

As to claim 4, McGarrahan et al. discloses the method wherein in verifying, the recipient is verified by externally contacting a licensing service with at least one of an identity of the recipient and an identification of the media stream (0033-0034, 0067-0068).

As to claim 5, McGarrahan et al. discloses the method wherein in sending, the authentication token includes limitations that instruct the media player to self destruct the media stream upon the occurrence of an event or pre-defined time (0053-0055).

6. Claims 15, 16, 18, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over McGarrahan et al. US Pub. 20030026424 A1. in view of Ishibashi et al. 20010053223 A1 and Spagna et al. 6859791 B1.

Regarding claim 15, McGarrahan et al. teaches the media content authentication system, comprising:

a distribution service for distributing media streams via streaming to recipients (fig. 1), wherein each media stream includes media content (0046, 0032-0033, and 0051) and a self-installing, the media content is in a format known only to the media player and the media player self-installs, self-loads, and self-executes when the recipients attempt to play the media content (0051; *user device STB displaying content stored with in STB based on authentication result upon user request*); and

an authentication service that subsequently communicates with each media player over a network in order to authenticate access to the recipients that attempts to play the media content (fig. 1 and 0054), and wherein each media player initiates the communication with the authentication service when it self-executes in an environment of a recipient to which it relates and each media player generates and supplies authentication information with the communication to the authentication service, the authentication information for a particular recipient to which a particular media player relates, and when authentication is successful each media player automatically plays media content included in the media stream (0051-0054).

One ordinary skill in the art would easily understand that authentication information of McGarrahan et al. is made of plurality of identifiers but fail to include few, Ishibashi et al. is disclosed for authentication information including identities for the recipients (*user ID*), identifications for the media content (*content ID*), identifications for the media streams, setting for each computing device's electronic environment, identifications for the media players

(*encryption processing unit ID*), identifications for any previous sender or previous recipient of the media streams, and identities for content providers that own the media stream (see fig. 16 of Ishibashi et al.).

McGarrahan et al. also fails to explicitly disclose wherein when the recipient receives the media content via the media stream the recipient receives with that media stream the media player (*media player/software, according to applicant's remark on 12/12/09, received with content at the recipient*), as amended.

However it is well known to transmit a content with a software to let the receiver/recipient device know what kind of software has been used (*see Ishibashi et al. fig. 5 for algorithms for signature..., and see fig. 12 a single stream 1200 that contains content and digital signature comprising algorithm, and see par. 0112, and 0130-0132 for verifying and providing content using the received algorithm*) using internet network to a user (see par. 0084 and 0101).

It would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Ishibashi within the system of McGarrahan et al. because they are analogous in content distribution. One would have been motivated to incorporate and modify the teachings, as Ishibashi suggests on 0204, to include any identification information for identification purpose in the authentication process.

Moreover, it would have been obvious at the time of the invention was made to modify the teachings of Ishibashi et al. within the system of McGarrahan et al. because they are analogous in secure method of providing content. One would have been motivated to modify the teachings because it would specify what kind of software has been used and authenticate using received algorithm.

Even though including any identifier within authentication information, such as an Internet Protocol (IP) addresses for computing devices of the recipients in the authentication information, is obvious to one ordinary skill in the art at the time of the invention, as explained above, the combination fails to disclose Internet Protocol (IP) addresses for computing devices of the recipients in the authentication information. However Spagna et al. is disclosed for receiving a content access request comprising IP address of the requester within authentication information and an authenticator comparing received IP address of the requestor with stored to provide the requested content access (see claim 16). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings within the combination system because it would control access to provide content.

Spagna et al. further discloses wherein the authentication token is a key pair having a private key of the media player known only to an authentication service and the media player and having a public key for the authentication server, wherein the authentication service is the method processing on the computer **(see col. 95 lines 5-15 and fig. 6 e.g. element 660 of fig. 6; sc(s) processor 192 of the end-user receives the content 113, decrypting the content 113 using the key 623, i.e. "content key" (see fig. 6 for key 623 being attached on the content), and also key 623 is a "key" corresponding to public key 661 *"it is decrypted using the Key 623 (corresponding to the Public Key 661) of the End-User(s) extracted from the license SC(s) sent from clearing house 105"* and therefor key 623 is a key pair, moreover key 623 is extracted from License SC(s) 660 received as a token transmitted via authenticator clearing house 105 and the content key 623 is a key that is only known by the clearing house and the end-user device).**

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to include the teachings of Spagna et al. within the combination system to use commonly known media private key and public key of the authenticator/content provider that is very well known in the art for security, at the time of the invention was made.

As to claim 16, McGarrahan et al. discloses the media content authentication system wherein each media player that self-installs contacts the authentication service immediately after it initially installs on a recipient's computing device (0051-0054).

As to claim 18, McGarrahan et al. discloses the media content authentication system wherein the authentication service uses a licensing service to authorize a number of the recipients for access to the media content (0033-0034, 0067-0068).

As to claim 19, McGarrahan et al. discloses the media content authentication system wherein the authentication service receives information from each of the media players that is used to authenticate each of the recipients, and the information includes at least one of settings of a computing environment that is executing the media player, an identity of the recipient, and an identification of the media content (0051-0054).

7. Claims 6-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over McGarrahan et al. US Pub. 20030026424 A1., Ishibashi et al. 20010053223 A1, Ishiguro et al. 7266691 B1.

and Spagna et al. 6859791 B1 and further in view of Yamasaki et al. US PUB. 2002/0161997 A1.

As to claim 6, the combination fails to disclose the method wherein in sending, the authentication token includes limitation that instruct the media player to prevent the recipient from re-streaming the media stream to a downstream recipient. However, preventing authorized user receiver tamper resistant device from transmitting content/content key to other unauthorized person is disclosed by Yamasaki et al. par. 0055 and fig. 3. Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the teachings of Yamasaki et al. within the combination system because they are analogous in content protection. One would have been motivated to do so because it would protect content from misappropriate use.

As to claim 7, Yamasaki et al. further discloses the method wherein in sending, the authentication token is at least one of a digital certificate and a digital signature (0015, 0042-0043, 0046 and 0048-0051). It would have been obvious to one having ordinary skill in the art at the time of the invention was made to use one of certificate/signature because it was very well known at the time of the invention to verify authorized content user in a system of content protection.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ELENI A. SHIFERAW whose telephone number is (571)272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Eleni A Shiferaw/

Examiner, Art Unit 2436